1. A method for re-establishing secure communications between a node and an endpoint node including the steps of:

copying, responsive to a reset at the node, a set of security associations stored in a memory to a working set of security associations, wherein the set of security associations includes only the security associations for endpoints nodes that are trusted by the node;

receiving, at the node, a communication from the endpoint node;

determining whether a security association for the endpoint node is included in the working set of security associations;

responsive to a determination that the security association for the endpoint node is in the working set of security associations, using the security association to process the communication from the endpoint node.

2. The method of claim 1, further including the step of verifying if the communication from the endpoint node is valid.

3. The method of claim 2, further including the steps of:

obtaining a new security association for the endpoint node responsive to a determination that the communication from the endpoint node is not valid; and

storing the new security association for the endpoint node in the working set of security associations.

4. The method of claim 1, further including the steps of:

obtaining a new security association for the endpoint node responsive to a determination that the security association for the endpoint node is not included in the working set of security associations; and

storing the new security association for the endpoint node in the working set of security associations.

5. A method of re-establishing communication between a node and an endpoint including the steps of:

storing an identifier of the endpoint on a trusted endpoint list;

negotiating a security association for the trusted endpoint, and storing the security association for the trusted endpoint in a working table of security associations; and

periodically copying a subset of the working table of security associations to a table of security associations in a memory.

6. The method of claim 5, further comprising the step of:

in the event of a reset, copying the table of security associations to the working table of security associations.

7. A network device including:

security association logic, coupled to the non-volatile memory, for applying security associations to communications received by the network device, the security association logic including:

a first memory comprising at least one entry, the entry comprising an endpoint identifier and a security association associated with the endpoint; and

a list of trusted endpoints; and

a second memory, storing a subset of data of the first memory.

8. The network device of claim 7, wherein the second memory is a non-volatile memory.

9. The network device of claim 7, further comprising means for periodically copying the subset of data of the first memory to the second memory.

10. The network device of claim 9, wherein the subset of data from the first memory that is copied to the second memory is selected responsive to the list of trusted endpoints.

11. The network device of claim 10 wherein only the entries of the first memory having endpoint identifiers that are on the list of trusted endpoints are copied to the second memory.

12. The network device of claim 7, further comprising means, responsive to a reset at the network device, for copying contents of the second memory to the first memory.